Computing Architecture

in Washington State Government

February 1994

Prepared by:
Washington State
Department of Information Services
PO Box 42440
Olympia, WA 98504-2440

Adopted by:
Washington State
Information Services Board

Computing Architecture
TABLE OF CONTENTS

Policies

Host Level Computing - Policy

Statutory Authority

RCW 43.105.041 (3) and (4) empower the Information Services Board (ISB) “to develop statewide or interagency policies, standards, and procedures” and to provide strategic planning goals and objectives for the state.

Purpose

To satisfy the statutory mandate, a comprehensive set of architectural standards for telecommunications, data, and computing will be developed. The first components of the computing architecture accompany this policy.

Objective

To migrate to a computing environment which promotes resource economies in information processing, optimizes use of scarce technical resources, provides increased opportunities for application transfer, and lowers the risk of technological obsolescence.

Applicability

The standards apply to all state agencies within the executive and judicial branches of state government. However, the initial focus will be on implementation of the standards in the executive cabinet agencies.

The standards do not apply to academic computing at Washington colleges and universities.

The host level computing architecture standards apply to administrative computing applications with large data and transaction volumes requiring significant staff support. Examples of large administrative computing applications include:

- Statewide systems such as the Agency Financial Reporting System and the Personnel Payroll System;

- Medical payment systems at the Departments of Social and Health Services and Labor and Industries;

- Drivers and Vehicles systems at the Department of Licensing;

- Benefit systems at the Employment Security Department; and

- Student, Financial, Purchasing, Budgeting, and Personnel Payroll Systems at the University of Washington and Washington State University.

Effective Date

This standard is effective for host level computing and software acquisitions or development efforts after September 27, 1990.

Policy Statement

State agencies shall comply with the host level computing architecture standards when acquiring computer hardware or software or contemplating significant application development efforts.

Exception Process

Departures from the standards require agency business case justification and Policy and Regulation Division approval.

Maintenance of the Standards

Technological advances and changes in agencies' business requirements will necessitate periodic revisions to standards adopted under this policy. The Policy and Regulation Division is responsible for evaluating the continued appropriateness of the standards. At a minimum, the Policy and Regulation Division will provide an annual status report on the existing architectural standards to the ISB. Major policy shifts require ISB approval

Adopting Architectural Standards - Policy

Statutory Authority

RCW 43.105.017(4)(a) states that the legislature intends through the establishment of the Department of Information Services (DIS) that "a structure be created . . . to plan and manage telecommunications and computing networks . . . ." RCW 43.105.041(3) empowers the Information Services Board (ISB) "to develop statewide or interagency technical policies, standards, and procedures . . . ."

Purpose

To satisfy the statutory mandate, a comprehensive set of architectural standards for telecommunications and computing are under development. The operating system, internetworking, and database management components of the computing architecture accompany this policy, supplementing existing standards for building wiring and cabling, and mainframe computing platforms (the 370 Standard).

Objective

To develop client/server computing that encourages connectivity, portability, scalability, and interoperability permitting an authorized computer user to access computer-based information resources anywhere in the state.

Applicability

This policy and its related standards apply to information technology systems acquired by agencies of state government under the information technology acquisition authority of the ISB.

Effective date

All information technology systems acquired after the effective dates specified in the individual standards must comply with those standards. Briefly, those effective dates are as follows:

- Operating Systems - September 1, 1991
- Internetworking - January 1, 1992
- Database Management Systems - January 1, 1992
- Electronic Mail - July 1, 1994

Policy Statement

State agencies shall comply with these standards. The standards are consistent with the ISB's stated vision of using open systems and a client/server model of computing, to facilitate access to the state's data resources regardless of where they reside.

Exception Process

Any departure from the approved architectural standards process must be accomplished through the process defined in the architectural exception policy. The Policy and Regulation Division of the Department of Information Services is responsible for routine maintenance of the standards to keep them current; only major policy shifts require ISB approval.

Exception Process - Policy

The architectural standards for information technology will be implemented over time through the state information technology planning, acquisition and feasibility study policies and processes. The Information Services Board (ISB) delegates no agency authority for information technology acquisitions that deviate from the architectural standards.

Waivers

Any information technology acquisition that deviates from the architectural standards requires the Department of Information Services (DIS), Policy and Regulation Division (PRD) review and approval. DIS will submit to the ISB for review those acquisitions that both deviate from the architectural standard and have agency or statewide impact, or a high degree of risk.

Requests for waivers must be in writing, signed by the top executive of the agency and the information processing manager and include written business case justification. Guiding principles to be used in the consideration of potential waivers include:

- Minimization of risk;
- Use of mainstream technology;
- Protection of investments in software and technical skills; and
- Improvement of connectivity

Situations that may lead to waivers include:

- Federal restrictions when funding of the acquisition is predominantly federal;
- Legislative or regulatory mandates requires exception measures;
- The standard would preclude the ability to transfer a system from another organization;
- Upgrades to the installed base of existing systems.

However, waivers shall generally be granted only if:

- Compliance with the standard would adversely affect the ability of the agency to accomplish mission critical functions; or

- Compliance would cause a major adverse financial impact on the agency which is not offset by statewide savings

Standards

Computing Architecture - Standards

Introduction to Computing Architecture Standards

Computing Architecture Standards is a collection of standards, recommendations, guidelines, and procedures to help agencies manage computing resources. The first in this set of standards is the Host Level Computing Architecture Standard. This standard is not meant to imply that all processing must occur at the host level.

With respect to all of the computing architecture standards:

- The standards apply prospectively.

- Application requirements and agency business needs are important considerations in evaluating the appropriateness of adherence to architectural standards in a particular situation. The standards are not expected to cover every situation.

- The burden of justifying exceptions to the standards rests with the requesting agency.

- To respond to the information processing needs of state government, the architectural standards will be reevaluated periodically.

Other components of the computing architecture to be addressed include standards for:

Work group computing:

- Desktop computing
- Information Technology planning
- Operations
- Tools
- Methods

For more information regarding the contents of the various components, please refer to *Statements of Direction: Computing Architecture.*

Background

The *Statements of Direction: Computing Architecture* provided the first step toward implementation of a standard state computing infrastructure. The *Statements of Direction* state that the intent of the ISB is to move to an "open systems architecture." An open, multi-tier combination of host-level computing, workgroup computing, and desktop computing is defined. This intent is reinforced by the *Information Technology Act of 1992* and the *Strategic Information Technology Plan of 1993.*

Host Level Computing Architecture - Standard

As adopted by the Washington State Information Services Board on September 27, 1990, the standard architecture for host level computing is:

- 370 Architecture;

- Presumptively using the MVS operating system and CICS teleprocessing monitor;

- For state government administrative information processing applications having large data and transaction volumes and requiring significant staff support.

Operating Systems - Standard

Objectives

The objectives of this operating system standard are to:

- Encourage portability and scalability of computer application programs;
- Encourage platforms that allow the easy installation of a wide range of existing applications;
- Increase the transferability of staff skills;
- Reduce the time required to port computer programs to different vendor hardware and architectures; and
- Ensure operating system compatibility and interoperability, thus maximizing the return on investment in generating or purchasing computer programs.

Strategy

To attain the above objectives, the state of Washington adopts the following standard:

- MS-DOS, OS/2, Windows (and their evolutionary family)
- UNIX

The VM operating system, while not listed as a standard product, is allowable when necessary to run more than one compliant operating system simultaneously on a 370 platform. VM is not approved for use in applications development.

The Macintosh Operating System is an allowable client operating system for executive or administrative office applications, but not large scale applications development purposes.

In addition to the products named above, certified POSIX.1 compliant products are acceptable.[1] To be POSIX.1 compliant, a vendor must show a Certification of Validation from the Computer Systems Laboratory of the
National Institute of Standards and Technology. Other acceptable evidence of POSIX.1. compliance is "branding," or certification, from X/Open demonstrating successful completion of the compliance tests.

Agencies should limit their purchases to vendors providing evidence of a corporate strategy to move toward POSIX.1 compliance whenever possible. POSIX.1 is the Federal Information Processing Standard (FIPS) described in FIPS Publication 151-2. The state of Washington standard will include

[1] POSIX.1. refers to the ISO/IEC Standard 9945-1 Portable Operating System Interface Part 1 System Application Program Interface [C language].

subsequent evolutionary POSIX.1 standards adopted by the Federal government, should FIPS Publication 151-2 be revised or superseded.

Published corporate statements of a direction toward POSIX.1 which establish target dates for release of POSIX.1 compliant products are acceptable evidence of a corporate commitment to POSIX.1 compliance.

Effective Date

September 1, 1991.

Applicability

This standard applies to operating systems that are developed or acquired for administrative use by state agencies. The standard is applicable to all computing platforms, including: micro or personal computers, mini-computers, workstations, and mainframes.

Conformance to the standard shall be required whether the operating system environments are:

- Internally developed by state employees;
- Developed for a state agency by an outside contractor;
- Acquired as part of an information system procurement;
- Acquired as a stand-alone information technology procurement; or
- Used under an information technology licensing or leasing arrangement.
- Solicitation documents must incorporate language requiring compliance with this standard from the effective date forward. Model language for
- Request for Proposals (RFP) is included in the appendix to the Acquisition Policy.

Other Information

This standard will be updated as needed to reflect changes in technology, trends in the industry, and government strategy. The existing standard will be subject to periodic review. Users and vendors will be included in the process of developing, implementing, reviewing and revising the standard.

A full copy of the POSIX.1 specification is available from the Institute of Electrical and Electronic Engineers (345 East 47th Street, New York, NY 10017) as IEEE Std. 1003.1-1990.

Internetworking - Standard

Objective

The objective of the Internetworking Standard is to establish consistent protocols for interconnecting computer networks. This will permit an authorized computer user to access computer-based information without limitation as to the physical location of that resource.

Definition

Internetworking: The connection of computers and networks of computers for the purpose of sharing information.

Protocol Suite: A collection of conventions for the interchange of information between computers and software.

Standard

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the required method of connecting between dissimilar networks.

When proprietary protocols are acquired, TCP/IP must also be acquired and loaded onto at least one computer, typically a network server.

All computers acquired by the state must be capable of running the TCP/IP protocol suite.

The TCP/IP protocol suite includes the networking protocols used in the Internet. The following protocols use TCP/IP and are the required minimum means of allowing remote users to transfer files and to log-in to applications that utilize a character-based display:

File Transfer	**Remote Log-in**
FTP	**Telnet** **TN3270**

The Telnet and TN3270 protocols allow users to log-in to and use applications on remote networks. Telnet is used for emulating VT100-type terminals; TN3270 is used for emulating IBM 3270-type terminals.

The full TCP/IP protocol suite includes many protocols other than TCP, IP, FTP, Telnet, and TN3270. This standard does not preclude the acquisition and use of these other components of the TCP/IP protocol suite as conditions and user requirements dictate. See also the related standard for electronic mail in this Policy Manual.

This Internetworking Standard does not preclude the acquisition or use of proprietary or copyrighted protocols within one or more networked clusters of computers that share the same network operating system protocols. However, TCP/IP *shall also be acquired* at the same time to preserve flexibility toward the state’s open systems direction. This is a requirement regardless of whether networks cross agency boundaries. Desktop computers and operating system software supporting server functions must use TCP/IP when internetworking.

Applicability

This standard concerns the accessibility and interoperability portions of a state open systems policy for information technology (IT). The result of this open systems policy will be a computing and communication infrastructure for the state of Washington that permits any state worker to access appropriate information and services regardless of:

- where those resources are located;
- the type of system providing them; and
- the type of computer the person is using.

This Internetworking Standard is intended to help agencies make an informed decision about acquiring IT resources. It specifies a protocol suite—or set of rules—for communicating between computers. Communication in this sense encompasses the ideas of accessibility and interoperability. While this standard does not address all facets of accessibility and interoperability, it does address the following:

Accessibility to:

- Other computers—Remote log-in to computers
- Other files—File transfer between computers

Interoperability between:

- Network Operating Systems

Figures 1 through 4 illustrate various configurations of networks and how this standard applies to them.

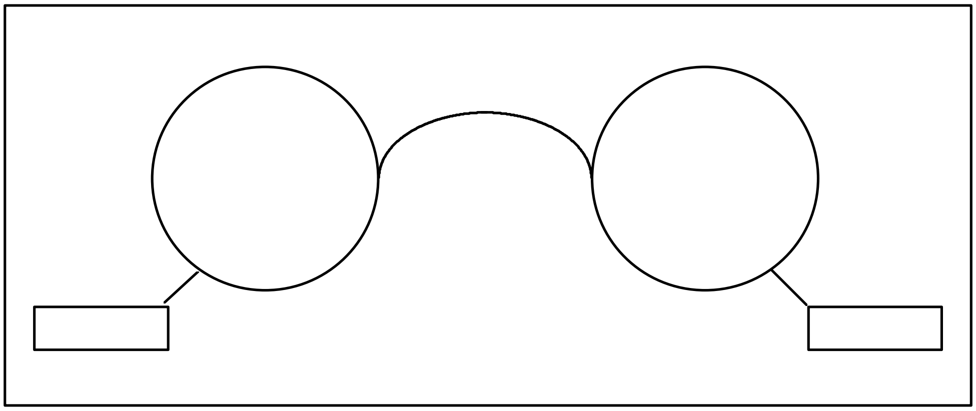

Figure 1 depicts a single agency with two network clusters both sharing the same Network Operating System (NOS) protocol, which will be referred to as “Protocol A.” The agency decides to connect the two networks. The agency may connect the two networks and continue to use Protocol A, but must also purchase TCP/IP software and install it on at least one server on each network cluster.

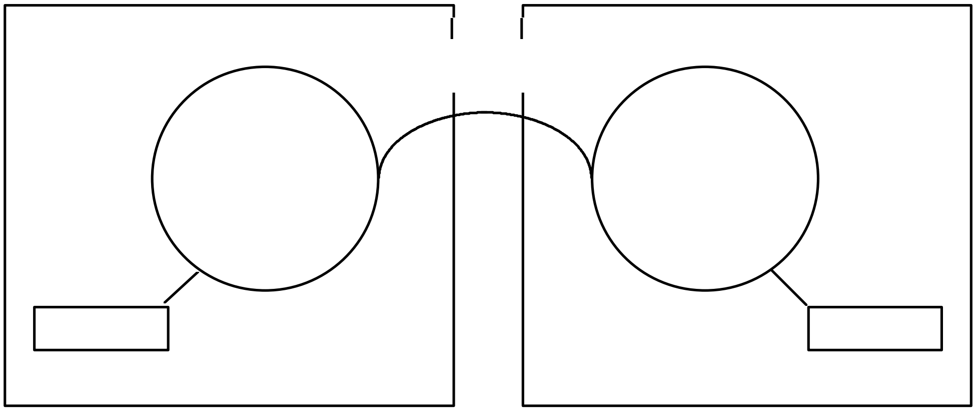

Figure 2 depicts two (or more) agencies with two network clusters both sharing the same Network Operating System (NOS) protocol, which will be referred to as “Protocol A.” The agencies decide to connect the two networks. The agencies may connect the two networks and continue to use Protocol A, but must also purchase TCP/IP software and install it on at least one server on each network cluster.

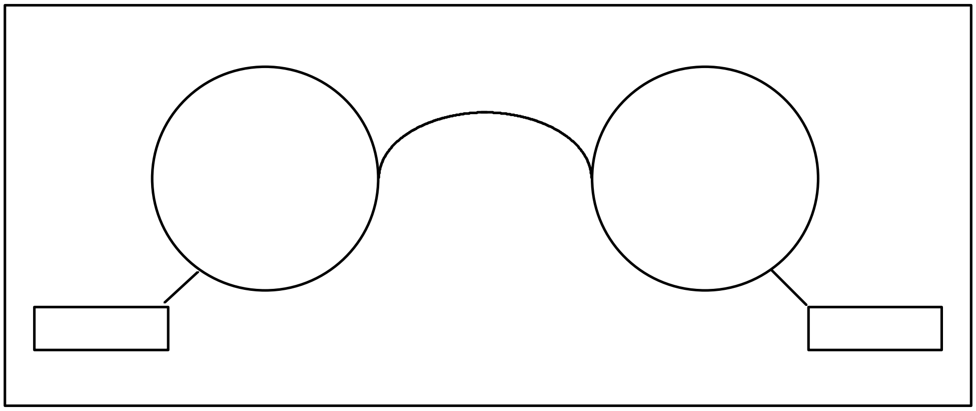

Figure 3 depicts a single agency with two network clusters that use two different Network Operating System (NOS) protocols, which will be referred to as “Protocol A” and “Protocol B.” The agency decides to connect the two networks. The agency must connect the two networks using the TCP/IP protocol suite by purchasing TCP/IP software and installing it on the servers that link the two networks.

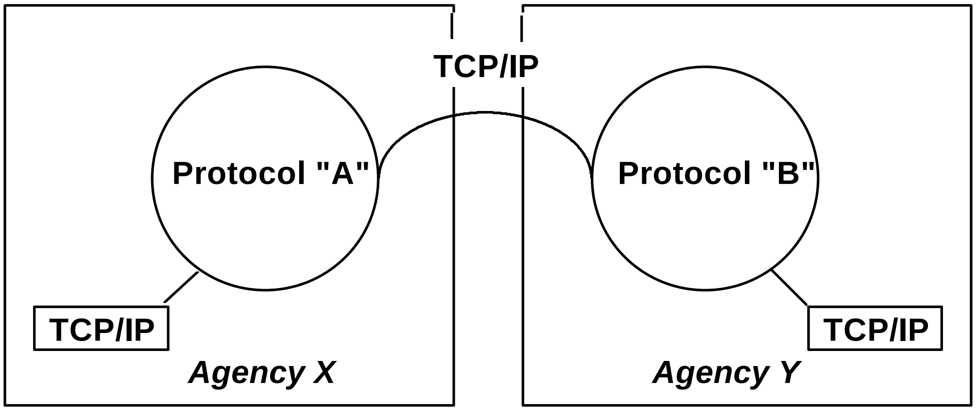

Figure 4: Multiple NOS Within Two Agencies

Figure 4 depicts two (or more) agencies with network clusters that use two different Network Operating System (NOS) protocols, which will be referred to as "Protocol A" and "Protocol B." The agencies decide to connect the two networks. The agencies must connect the two networks using the TCP/IP protocol suite by purchasing TCP/IP software and installing it on the servers that link the two networks.

Organizations must use Telnet and/or TN3270 when they elect to allow users on remote networks using different protocols to access applications which support these types of devices. This standard is not meant to require the development of video displays for these or other character-based display devices. Rather, if such an application supports VT100 or 3270-type devices, Telnet and/or TN3270 shall be used to allow remote access.

Terminology

FTP:	File Transfer Protocol
NOS:	Network Operating System
TCP/IP:	Transmission Control Protocol/Internet Protocol
Telnet:	Process allowing remote log-in to hosts
TN3270:	3270 Terminal Emulation
VT100:	Video Terminal 100 emulation (often a default emulation)

Strategy

This Internetworking Standard is consistent with the Washington State Information Services Board's (ISB) stated vision of using open systems standards as they apply to distributed computing resources on various computer networks to facilitate access to the state's data resources regardless of where they might reside.

Open systems refers to standards-backed, vendor-neutral IT products. Open systems encourage interoperability in a heterogeneous computing environment. Two attributes are required for a standard to be a candidate for the open systems designation:

- the content of the standard, or specification, must be under the control of a recognized and accredited standards body or a recognized industry consensus group; and

- the standard must have been arrived at in a public, consensus-based process.

Agencies shall use the TCP/IP protocol suite in assessing the acquisition or development of internetworking functions for IT projects.

Creation of the Internetworking Standard is a starting place, not an end result. Technological advances and changes in the business requirements of the state will necessitate periodic revisions to the standards adopted under this policy. The Policy and Regulation Division of the Department of Information Services is responsible for keeping the routine maintenance of standards current; only major policy changes will require ISB approval.

Effective Date

TCP/IP is the enabling standard for internetworking computer systems acquired by the state on or after January 1, 1992. All computers acquired after January 1, 1992, must have the ability to run the TCP/IP protocol suite. Computers can be capable of operating several different protocols as long as one of them is TCP/IP.

Database Management Systems - Standard

Introduction

This standard recognizes that there are different types of database management systems (DBMS). For purposes of this standard, types of DBMS technology will be classified as:

- Traditional
- Relational
- Emerging or non-traditional

While the standard refers to relational databases, it does not recommend that be the only type of database considered when making database decisions. The standard also recognizes that emerging or non-traditional technologies will provide a requirement to periodically evaluate and update the standard. How this standard applies to these different types of DBMS is addressed in the sections on strategy and applicability.

Objectives

The overall objective of this standard is to facilitate the sharing of data, promote the portability and scalability of database application programs, and improve transferability of programming staff and skills within and among state agencies.

The state of Washington computing environment is a diverse collection of hardware, operating systems, applications programs and languages, and database management systems. This standard expects to increase interoperability between and among databases through the use of a standard database access language.

Strategy

To attain the above objectives, the state of Washington adopts the following standard:

As of January 1, 1992, purchases of administrative relational database products are limited to those products that implement the Database Language SQL standard described in the Federal Information Processing Standard (FIPS) Publication 127-2. The state of Washington standard will incorporate subsequent evolutionary SQL standards adopted by the federal government, should FIPS Publication 127-2 be revised or superseded.

To be acceptable as *conforming to the SQL standard,* the product must have been issued a registered Validation Summary Report from the Computer Systems Laboratory of the National Institute of Standards and Technology (NIST) indicating successful completion of compliance tests *or* a written statement must be issued by the vendor stating that they are in the process of being certified. It is in an agency’s best interest to independently verify the claim of certification-in-process. Upon submission for validation, the Computer Systems Laboratory sends the vendor a letter acknowledging the request for validation and indicating the month scheduled for validation testing. This letter can be used as proof of vendor commitment to the testing process.

A *Validated Processor List* is published quarterly by NIST. An example of this list is included in Appendix A of this standard. DIS Policy and Regulation Division will maintain the most recent version of the list on file and will provide copies on request. The list is also available via anonymous FTP from NIST at the following file server address:

speckle.ncsl.nist.gov

Conformance to FIPS SQL requires a Module Language or Embedded SQL interface to one or more of the following languages: Ada, C, COBOL, FORTRAN, or Pascal.

Solicitation documents must incorporate language requiring SQL compliance from the effective date forward. Model Request for Proposal (RFP) language is included in the Model RFP appended to the Information Services Board Policy “Acquisition and Disposal of Information Technology Resources.”

Purchases of administrative traditional database products after January 1, 1992 will be limited to the installed base of DBMS products as of September 1991 that:

- Reside on established 370 host level computing platforms (installed products as of that date are ADABAS and IMS); or

- Reside on departmental processors and currently support mission critical applications within state government; or

- Reside on microcomputers and are identified in the agency Information Technology Plan as the agency micro DBMS standard.

This standard applies to all administrative relational database applications developed or acquired by state agencies after January 1, 1992, to support mission critical applications within state government. The standard is applicable to all computing platforms, including: personal computers, workstations, minicomputers (both departmental and stand-alone), database servers and mainframes.

Data access using the SQL call structure is best suited for use in accessing relational databases and applications that use the relational data model. Further, the use of the standard SQL is strongly recommended for any database access when one or more of the following situations exist:

- The expected life of the database application is longer than the life of the current equipment or database management system, if any.
- There may be frequent changes to the database application or its specifications.
- The physical database is being designed and developed centrally for a decentralized system using different makes and models of computers or database software from a different vendor.
- It is expected that the database application may be run under a database management system other than the one for which it was initially written.
- Maintenance of the database application will be performed by programmers other than those who developed it.
- The data is likely to be used by other agencies or other governments.

There may be times when agency requirements can be met more economically and efficiently by the use of automatic program generators or by database access through a high level language system. However, if the final output of the program generator or high-level language system will require access to a relational database, then the conditions and specifications of SQL are to be adhered to.

Emerging or non-traditional database applications such as imaging, multimedia, hypertext, object-oriented, or scientific data collection are currently excluded from the applicability of this standard. To the extent that emerging technology products have SQL capability, SQL capable products are preferred over non-SQL capable products.

Effective Date

January 1, 1992

Other Considerations

Many vendors provide proprietary extensions to their SQL product to differentiate it from the SQL products of other vendors. Nonstandard SQL features should be used only when the needed operation or function cannot be reasonably implemented with the standard features.

The use of nonstandard features can make the interchange of programs or the replacement of a database management system more difficult and more costly. This standard defers implementation of the FIPS Flagger requirement for development or acquisition of Washington State database applications. The requirement to “flag” nonstandard features will be evaluated during the annual review of this standard.

Electronic Mail - Standard

Objective

The objective of the Electronic Mail Standard is to permit the open exchange of information among employees of the state of Washington, vendors, other government organizations, and members of the general public. Ideally, electronic mail allows the exchange of information without regard to the specific model or brand of computer software or hardware used by either the sender or recipient of electronic mail messages and attachments.

Definition

Electronic Mail: The exchange and distribution of messages, documents, graphics, data and other information in electronic form between users of computers.

Standard

Electronic mail systems acquired by the state must be capable of exchanging mail messages and attachments using the following protocols and formats:

SMTP	Simple Mail Transport Protocol
RFC-822	Request For Comment #822
MIME	Multipurpose Internet Mail Extension

The above standards define the required, minimum means of exchanging electronic mail messages and attachments between dissimilar systems. This standard does not preclude the acquisition and use of other electronic mail messaging protocols and formats in addition to these. However, the above items must be supported as well as any other protocols and formats supported by a particular product.

Applicability

This standard concerns the accessibility and interoperability portions of a state open systems policy for information technology (IT). The result of this open systems policy will be a computing and communication infrastructure for the state of Washington that permits any state worker to access appropriate information and services regardless of:

- where those resources are located;
- the type of system providing them; or
- the type of computer the person is using.

This Electronic Mail Standard is intended to help agencies make an informed decision about acquiring electronic mail as an IT resource. It specifies standards to enable compatibility between electronic mail software packages. It uses standards accepted by the Internet community as the technology model upon which the state’s standards are based.

This Electronic Mail Standard applies to all software systems acquired or developed for the purpose of exchanging electronic mail messages and attachments. The standard applies regardless of whether an electronic mail package will be used solely for exchange of messages within an organization, between agencies, or among organizations and individuals outside of state government.

Strategy

This Electronic Mail Standard is consistent with the Washington State Information Services Board's stated vision of using open systems standards as they apply to distributed computing resources on various computer networks to facilitate access to the state's data resources regardless of where they might reside.

Open systems refers to standards-backed, vendor-neutral IT products. Open systems encourage interoperability in a heterogeneous computing environment. Two attributes are required for a standard to be a candidate for the open systems designation:

- the content of the standard or specification must be under the control of a recognized and accredited standards body or a recognized industry consensus group; and

- the standard must have been arrived at in a public, consensus-based process.

Agencies shall use the Electronic Mail standards in assessing the acquisition or development of electronic mail functions for IT projects.

Creation of the Electronic Mail Standards are a starting place, not an end result. Technological advances and changes in the business requirements of the state will necessitate periodic revisions to the standards adopted under this policy. The Policy and Regulation Division of the Department of Information Services is responsible for keeping the routine maintenance of standards current; only major policy changes will require Board approval.

Effective Date

Electronic mail systems acquired by the state after January, 1994 must support the SMTP protocol and RFC-822 specification for message formats. Electronic mail systems acquired by the state after July, 1994 must support the MIME specification for mail attachments.

Guidelines

Internetworking Implementation Guidelines

Implementation

The Internetworking Standard describes a required set of protocols for internetworking among heterogeneous computers. The Standard applies only to those networks of computers communicating with other networks of computers. However, a full implementation of the Standard consistent with the direction and intent of open systems policies to enable access to information and services for all state workers would encompass the following recommended guidelines.

- Stand-alone desktop computers used for internetworking should be equipped with TCP/IP, Telnet, and FTP software. All servers should have a protocol stack loaded with TCP/IP, Telnet, and FTP software. Servers should be capable of downloading the TCP/IP protocol suite to resident memory on networked desktop computers.

- Client/server applications should be designed to work in a TCP/IP network environment.

- Information providers should enable appropriate access to their systems from all key desktop computer-types via TCP/IP-based services.

- Desktop computers should have access to a direct Internet Protocol (IP) path (without any protocol translation) to the Internet to facilitate access to the information resources available there.

Technical Considerations

Most Local Area Networks (LANs) were developed to provide a simple medium for personal computers to share resources. The role of the LAN is changing into a complex inter-system communications link. Personal computers now share the LAN with multi-user mini-computers, communications controllers, terminal servers, and even mainframes. TCP/IP is a single, compatible communications protocol suite that enables resource sharing in this complex internetworked environment.

The TCP/IP protocol builds on existing technology. Ethernet, X.25, FDDI, and Token Ring are data link standards, methods of getting a packet of data from one computer to another. The lowest layer of the TCP/IP protocol suite, the Internet Protocol (IP), operates above the data link. IP provides a way of linking sub-networks. The IP module takes a packet from one data link, consults a routing table and forwards it to another data link. For this to work, each node (workstation, server, router, or gateway) must have a unique address (see Addressing below).

The transport layer provides user-to-user delivery service and resides on top of the IP network layer. The transport layer decides to which user an incoming packet from the network layer belongs. It may also feature value-added services such as guaranteed delivery.

There are two basic transport layer protocols within the TCP/IP protocol suite: User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). UDP serves an end user with a very low overhead transport service but does not guarantee that the data will be delivered. TCP is known as a stream-oriented service provider that guarantees that all data submitted to TCP at one end of the network will emerge error free at the other end and in the order it was sent.

There are a variety of services to run on top of TCP/IP. Three basic ones are Telnet, file transfer protocol (FTP), and Simple Mail Transfer Protocol (SMTP). FTP is a way to copy a file from one computer to another. Telnet allows an interactive log-on to a remote computer providing simple terminal emulation and limited graphics. SMTP sends mail messages.

Addressing

Each node (workstation, server, router, or gateway) on an IP-based network must have a *unique* address. Users assign IP addresses to these devices at the time that the devices are initially configured and installed on a network. But because users can assign addresses, the possibility exists of duplicate addresses being created. Serious problems with network reliability may result from two devices with the same address operating on the same network. One way to avoid this problem is to request addresses from a central registration authority who guarantees uniqueness for all addresses it has registered. The Defense Data Network - Network Information Center, located at Network Solutions, Inc., provides such a service. The Information Center has the authority to delegate the registration of sites. The Information Center can be contacted at:

Network Solutions, Inc.
Attn: Network Information Center
14200 Park Meadow Drive, Suite 200
Chantilly, Virginia 22021
Tel: 800-365-3642; 703-802-4535
Fax: 703-802-8376
Internet e-mail: hostmaster@nic.ddn.mil

The Information Center assigns only the network portion of the address. The individual site must then establish and register a new domain name by returning an application to the Information Center.

IP addresses (e.g., 147.55.208.34) are mapped to names written in the Domain Name System (DNS) format. The first part of the IP address in DNS format represents the name of a network host; the rest of the name represents sub-domains and domains. For example, the IP address 147.55.208.34 written in DNS format as dis.wa.gov refers to a host.subdomain.domain: “dis” is the host name; “gov” is the domain for non-military government entities; and “wa” is a second-level domain that is uniquely registered. The complete Internet address of a particular user would include the user’s identification (user-id) as follows: *jq_public@dis.wa.gov*.

Under the management of a domain administrator, the second-level domain may be subdivided into third-level domains, fourth-level domains, and so forth. This means that agencies wishing IP connectivity need not necessarily register with the Information Center and establish their own unique IP address *if* another service provider has agreed to subdivide its unique sub-domain.

The following is a summary of current top-level domains:

.com	commercial businesses and organizations
.edu	educational and research institutions
.gov	non-military government organizations
.mil	US military organizations
.net	Internet backbone systems
.org	not-for-profit organizations
.us	home computers, small companies, other
.int	special international organizations

Security

The objective of the Internetworking Standard is to permit an authorized computer user to access any appropriate computer-based information resources. Use of TCP/IP as a standard computer communications protocol will increase access to state information resources. Data security in this environment remains the responsibility of each agency. Agencies shall determine the rules for network access to information within their control.

Cost Components

The ISB recognizes that interoperability among computers acquired by government organizations justifies some level of expenditure.

The following factors should be considered in determining internetworking cost:

- Protocol costs;
- Hardware costs (including additional memory requirements for workstations);
- Software costs; and
- Support costs (including address pool management).

Further Information

The Request For Comment series of documents available from NSFNET Network Service Center provides an excellent, timely resource for TCP/IP information. On Internet send mail to: *info-server@sh.cs.net*

Appendix A

This appendix contains excerpts from the *Programming Languages and Database Language SQL Validated Processor List* 1994 No. 1 from the U.S. Department of Commerce National Institute of Standards and Technology National Computer Systems Laboratory.

Example of SQL Validated Processor List